

(Use several sheets if necessary)

FILING DATE
January 16, 2002

**GROUP
2136**

[illegible][illegible]

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)		
Dee		R. L. Rivest, et al "A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, vol. 21, No. 2. pp. 120-126, 1978.
Dee		V. S. Miller, Use of elliptic curves in Cryptography, Proc. of Crypto '85, LNCS218, Springer-Verlag, pp. 417-426, 1985.
Dee		N. Koblitz, Elliptic Curve Crytosystems, Math. Comp. 48, 177, pp. 203-209, 1987.

DATE CONSIDERED

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(Use several sheets if necessary)

10/046,224

FILING DATE
January 16, 2002

**GROUP
2136**

[illegible][illegible]

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)	
✓	M. O. Rabin, Digital Signatures and Public-key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCSTRANSMISSION-212, 1979.
✓	T. El Gamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE, Trans. on Information Theory, IT-31, 4, pp. 469-472, 1985.
✓	S. Goldwasser, et al Probabilistic Encryption, JCSS, 28, 2, pp. 270-299, 1984.

DATE CONSIDERED

1/31/2006

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(Use several sheets if necessary)

FILING DATE
January 16, 2002

10/046,224

**GROUP
2136**

[illegible]

FOREIGN PATENT DOCUMENTS										DATE	COUNTRY	CLASS	SUBCLASS	ABSTRACT	
DOCUMENT NUMBER													YES	NO	

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)	
Doc	M. Blum et al, An Efficient Probabilistic Public-key Encryption Scheme which hides all Partial Information, Proc. of Crypto '84, LNCS196, Springer-Verlag, pp. 289-299, 1985.
Doc	S. Goldwasser, et al, Lecture Notes on Cryptography, http://www-cse.ucsd.edu/users/mihir/1997 .
Doc	T. Okamoto, et al, A new Public-key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt '98, LNCS1403, Springer Verlag, pp. 308-318, 1998.

EXAMINER

DATE CONSIDERED

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(Form PTO-1449 [6-4])

(Form PTO-1449 [6-4])

(Use several sheets if necessary)

500.41092X00

SERIAL 10/046,224

APPLICANT
M. NISHIOKA, et al

FILING DATE
January 16, 2002

**GROUP
2136**

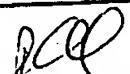

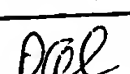
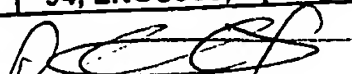
U.S. PATENT DOCUMENTS

[illegible]

FOREIGN PATENT DOCUMENTS

[illegible]

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)	
	D. Dolve, et al Non-Malleable Cryptography, In 23 rd Annual ACM Symposium on Theory of Computing, pp. 542-552, 1991.
	M. Naor, et al Public-key Cryptosystems Provably Secure Against Chosen Ciphertext Attacks, Proc. of STOC, ACM Press, pp. 427-437, 1990.
	M. Bellare, et al "Optimal Asymmetric Encryption How to Encrypt with RSA, Proc. of Eurocrypt '94, LNCS950, Springer Verlag, pp. 92-111, 1994.
EXAMINER 	DATE CONSIDERED 1/31/2006

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(Form PTO-1449 [6-4])

(Form PTO-1449 [6-4])

(Use several sheets if necessary)

**GROUP
2136**

[illegible][illegible]

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)	
ll	R. Cramer et al, A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack, Proc. of Crypto '98, LNCS1462, Springer-Verlag, pp. 13-25, 1998.
ll	M. Bellare, et al Relations Among Notions of Security for Public-key Encryption Schemes, Proc. of Crypto '98, LNCS1462, Springer Verlag, pp. 26-45, 1998.

1/31/2006

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.